Digital Forensics in Communication Systems
(Цифровая криминалистика в системах связи)

Educational review paper

Author:
Viktor Afanasiev

Academic degree:
Bachelor of Engineering
(Automation and Control Systems)

Field of study:
Telecommunications engineering
Digital forensics
Incident analysis in communication systems

Year:
2025

аннотация

В работе рассматривается применение методов цифровой криминалистики в инженерной практике телекоммуникаций и связи. Цифровая криминалистика пр

Особое внимание уделено анализу цифровых следов, формирующихся в процессе функционирования телекоммуникационных систем: данным файловых систем

Целью работы является формирование у обучающихся системного инженерного мышления в области анализа инцидентов и цифровых угроз в телекоммуника

Работа носит учебно-аналитический характер и ориентирована на студентов и специалистов инженерных направлений в области связи и телекоммуникац

---

Введение

Современные телекоммуникационные системы представляют собой сложные распределённые инфраструктуры, включающие аппаратные средства, программные

Традиционный эксплуатационный подход, ориентированный исключительно на устранение последствий, в условиях высокой сложности инфраструктуры ока

Цифровая криминалистика в данном контексте рассматривается как совокупность методов анализа цифровых следов, формирующихся в процессе функцион

Актуальность данной работы обусловлена необходимостью подготовки универсальных инженеров связи, способных работать на стыке эксплуатации, анал

Целью данной учебно-аналитической работы является формирование у обучающихся целостного представления о применении методов цифровой криминалис

Таким образом, введение задаёт теоретическую и методологическую основу для последующего изложения материала, учебных модулей и заключительных

1. анализ цифровых инцидентов задачи инженера

Цифровая криминалистика в инженерной практике телекоммуникаций используется не как отдельная дисциплина и не как юридический инструмент рассле

Любой анализ начинается с фиксации состояния системы. В телекоммуникационной инфраструктуре это означает создание точной копии носителей данны

Восстановление данных в инженерной практике используется не для возврата информации как таковой, а для выявления следов вмешательства и измене

Файловая система в телекоммуникационных системах отражает поведение инфраструктуры во времени. Анализ изменений дат, структуры каталогов и лог

Оперативная память представляет собой особую зону анализа, так как многие процессы и соединения существуют исключительно в RAM. Для фиксации с

Мобильные устройства всё чаще используются как элементы управления телекоммуникационной инфраструктурой. Анализ разблокированных устройств поз

Сетевой трафик является ключевым носителем следов в телекоммуникациях. Любая аномалия — отказ, перегрузка или атака — проявляется в потоках да

Логи и журналы формируют временной скелет инцидента. Без сопоставления событий во времени невозможно установить причинно-следственные связи. В

Видео- и аудиоданные часто используются в телекоммуникационной инфраструктуре как вспомогательные источники информации — диспетчерские записи,

Документы и сопутствующие метаданные являются источником управленческих и эксплуатационных следов. Сравнение версий документов с помощью DiffP

Встроенные устройства и прошивки представляют скрытую зону риска в телекоммуникационной инфраструктуре. Анализ прошивок с использованием Binwa

OSINT-инструменты расширяют инженерный анализ за пределы локальной инфраструктуры. Maltego Community и SpiderFoot HX в Windows-среде, а также

Инструменты искусственного интеллекта применяются как вспомогательный аналитический слой. OpenCV, TensorFlow, PyTorch и scikit-learn использую

В совокупности криминалистический подход формирует у инженера связи системное видение инфраструктуры. Система воспринимается как динамический

2. учебно-практический модуль

В основной статье были рассмотрены классы инструментов цифровой криминалистики, инженерного анализа и расследования инцидентов: средства фикса

Учебный блок, представленный ниже, предназначен для устранения этого разрыва. Его задача — показать единый рабочий цикл, в котором инструменты

---

Учебный модуль: практический цикл анализа инцидента

(от фиксации состояния до аналитического вывода)

Исходная инженерно-криминалистическая ситуация

Рассматривается типовая, но показательная ситуация. На рабочем компьютере или ноутбуке зафиксированы признаки нарушения нормального функционир

Цель специалиста в данной ситуации — не устранить проблему, а понять, что именно произошло, в какой последовательности, с какими последствиями

---

Этап 1. Фиксация состояния системы как отправная точка анализа

Работа начинается с фиксации текущего состояния носителей информации. Для этого используются средства побайтового копирования: FTK Imager в ср

Практическое действие заключается в создании образа диска с одновременной фиксацией контрольных сумм. После этого оригинальный носитель выводи

Аналитическое значение этого этапа заключается в том, что специалист получает стабильную точку отсчёта. Любые выводы, сделанные далее, опираются

---

Этап 2. Первичный обзор структуры данных и ориентирование

На следующем этапе образ монтируется в режиме «только для чтения» с помощью OSFMount или аналогичных средств. Далее используется Autopsy как и

Практическая задача этапа — ориентирование. Специалист отмечает зоны, потенциально значимые для дальнейшего анализа: нетипичные каталоги, необ

Аналитически это позволяет избежать хаотичного анализа. Вместо бессистемного просмотра файлов формируется карта исследования, на основе которо

---

Этап 3. Анализ удалённых данных как индикатор вмешательства

После ориентирования внимание переключается на анализ удалённых данных. Используются PhotoRec, Recuva, TestDisk или аналогичные инструменты. Ц

Практически специалист анализирует количество обнаруженных удалённых фрагментов, их временные метки и распределение по файловой системе. Эти д

Аналитический вывод заключается в том, что удаление данных рассматривается как событие, требующее объяснения. Даже если содержимое файлов восс

---

Этап 4. Построение временной линии событий

На этом этапе данные из предыдущих шагов объединяются во времени. Используются Plaso (log2timeline) для агрегации журналов и Timesketch для ви

Практическая работа заключается не в механическом построении таймлайна, а в его анализе. Специалист ищет узловые точки: первое аномальное собы

Аналитическое значение временной линии состоит в том, что она позволяет отделить причину от следствия. Многие ошибки анализа возникают именно

---

Этап 5. Анализ сетевой активности как внешнего канала информации

После восстановления внутренней хронологии внимание переключается на сетевое взаимодействие. С помощью Wireshark и NetworkMiner анализируются

Практически специалист не стремится расшифровать весь трафик. Основное внимание уделяется шаблонам: регулярные соединения, нестандартные порты

Аналитически сеть выступает в роли внешнего свидетеля. В отличие от файловой системы, сетевой трафик отражает взаимодействие системы с окружаю

---

Этап 6. Формирование аналитического заключения

Финальный этап заключается в синтезе результатов. Специалист не перечисляет найденные файлы и не описывает инструменты. Он формирует связное о

Важно подчеркнуть, что заключение не является юридической оценкой. Оно представляет собой инженерно-аналитическое описание фактов, пригодное д

---

Общий аналитический вывод учебного блока

Практический анализ инцидента невозможен при использовании инструментов по отдельности. Каждый инструмент даёт лишь фрагмент информации, котор

Именно такой подход превращает специалиста из «пользователя программ» в инженера-аналитика, способного работать с неопределённостью, восстанав

Учебная практика. Модуль 2

Анализ мобильных устройств в рамках инженерно-криминалистического подхода

Место мобильных устройств в общей логике анализа

Мобильное устройство в современных инцидентах редко является изолированным объектом. В большинстве случаев оно выступает либо как продолжение

Принципиально важно рассматривать смартфон не как носитель файлов, а как динамическую систему, совмещающую в себе вычислительную среду, сенсор

---

Исходная ситуация

В рамках расследуемого инцидента выявлено, что пользователь активно использовал мобильное устройство в тот же временной интервал, когда происх

Задача специалиста — определить:

факт участия мобильного устройства;

характер этого участия;

связь с другими элементами системы.

---

Этап 1. Фиксация состояния мобильного устройства

Анализ мобильного устройства начинается не с приложений и не с сообщений. Первое, что должен сделать специалист, — зафиксировать текущее состо

В зависимости от платформы используются ADB (Android), libimobiledevice (iOS), а также средства логического извлечения данных, такие как AFLog

Практическая задача этапа — получить логическую копию доступных данных без вмешательства в пользовательскую среду и без обхода механизмов защи

Аналитический вывод:

На этом этапе специалист ещё не «извлекает доказательства», а сохраняет контекст использования устройства, который может быть утрачен при даль

---

Этап 2. Анализ пользовательской активности

После фиксации проводится анализ пользовательских артефактов: журналов вызовов, сообщений, активности приложений, временных меток. Здесь важно

Практически специалист сопоставляет:

периоды активности телефона;

моменты сетевых подключений;

совпадение этих событий с временной линией, построенной ранее для других систем.

Например, всплеск активности мессенджера или VPN-клиента может совпадать с моментом передачи данных с рабочего компьютера.

Аналитический вывод:
Мобильное устройство часто выступает триггером или подтверждением событий, происходящих в других системах. Даже без чтения содержимого сообщен

---

Этап 3. Сетевое взаимодействие мобильного устройства

Мобильное устройство почти всегда активно взаимодействует с сетью. Анализ сетевых артефактов включает:

историю подключений Wi-Fi;

использование мобильных данных;

признаки работы прокси, VPN или туннелей.

Практическое использование заключается в выявлении точек выхода устройства во внешнюю среду и сопоставлении этих точек с сетевой активностью,

Аналитический вывод:
Смартфон нередко служит мостом между изолированными средами, и его сетевые артефакты позволяют восстановить направление и характер взаимодейст

---

Этап 4. Оперативная память и временные данные (при наличии)

В редких, но значимых случаях применяется извлечение данных оперативной памяти (LiME для Android). Это оправдано, если существует подозрение н

Практически это позволяет выявить:

активные процессы;

временные сетевые соединения;

данные, не сохранённые в постоянной памяти.

Аналитический вывод:
Как и в случае с настольными системами, ОЗУ отражает моментальную реальность, которая может исчезнуть при перезагрузке или блокировке устройст

---

Этап 5. Интеграция данных мобильного устройства в общую картину

Финальный этап анализа мобильного устройства заключается не в отдельном отчёте, а во включении его данных в общую временную и причинно-следств

событиями на стационарных системах;

сетевой активностью;

действиями пользователя.

Аналитический вывод:
Ценность мобильного анализа проявляется не в изоляции, а в способности подтвердить, уточнить или опровергнуть гипотезы, выдвинутые на других э

---

Учебная практика. Модуль 3

Типовые ошибки анализа и ложные выводы

Почему этот модуль необходим

Большинство ошибок в цифровом анализе связано не с неправильным использованием инструментов, а с неверной интерпретацией полученных данных. Эт

---

Ошибка 1. Анализ без фиксации исходного состояния

Распространённая ошибка — начинать анализ «на живой системе», открывая файлы и приложения. Это приводит к изменению временных меток и разрушен

Вывод:
Любой анализ без предварительной фиксации данных превращается в субъективное исследование.

---

Ошибка 2. Изолированное использование инструментов

Использование одного инструмента без сопоставления результатов с другими источниками часто приводит к ложным выводам. Например, обнаружение уд

Вывод:
Инструменты дают данные, но не дают смысла.

---

Ошибка 3. Подмена корреляции причинностью

Совпадение событий во времени не всегда означает причинно-следственную связь. Частая ошибка — объявлять процесс «виновным» только потому, что

Вывод:
Временная близость — это повод для анализа, а не доказательство.

---

Ошибка 4. Игнорирование человеческого фактора

Автоматизация и системы логирования не отменяют человеческого поведения. Ошибки пользователей, непонимание процессов, случайные действия могут

Вывод:
Система отражает не только атаки, но и поведение человека.

---

Ошибка 5. Избыточная вера в автоматизацию и ИИ

Использование ИИ-инструментов без критического контроля может привести к формированию ложных акцентов. Автоматическая классификация не заменяе

Вывод:
ИИ — это усилитель внимания, а не источник истины.

---

Общий вывод раздела «Учебная практика»

Практическое применение инструментов цифровой криминалистики и инженерного анализа требует не столько знания программ, сколько умения выстраив

Учебные кейсы для студентов и методистов

Назначение блока

Настоящий блок предназначен для закрепления материала, изложенного в предыдущих модулях учебной практики. Кейсы не предполагают единственного

Кейсы могут использоваться:

в учебных занятиях;

при самостоятельной работе студентов;

в качестве основы для обсуждений и защиты аналитических выводов;

при подготовке методических материалов.

---

Кейс 1. «Пропавшие документы»

Исходная ситуация.
Сотрудник утверждает, что важные рабочие документы исчезли с его компьютера. Он отрицает удаление файлов и предполагает «сбой системы».

Данные для анализа.
В распоряжении специалиста:

образ диска рабочей станции;

журналы событий операционной системы;

сведения о рабочем графике пользователя.

Задача обучающегося.
Определить:

имело ли место удаление данных;

носит ли удаление системный или пользовательский характер;

какие этапы анализа необходимо провести в первую очередь.

Ожидаемая логика рассуждений.
Студент должен показать понимание того, что:

отсутствие файла не тождественно его уничтожению;

анализ начинается с фиксации и построения временной линии;

вывод делается на основе совокупности артефактов, а не одного признака.

Методический комментарий.
Кейс проверяет способность отличать факт события от его интерпретации и формировать гипотезы, а не обвинения.

---

Кейс 2. «Чистый диск и подозрительная активность»

Исходная ситуация.
На рабочем компьютере не обнаружено подозрительных файлов. Однако сетевой администратор зафиксировал нестандартную сетевую активность.

Данные для анализа.
Доступны:

дамп оперативной памяти;

журналы сетевых соединений;

временная линия системных событий.

Задача обучающегося.

Предложить последовательность анализа и объяснить, почему файловая система может не отражать фактическую активность.

Ожидаемая логика рассуждений.
Студент должен:

указать на роль оперативной памяти как источника временных данных;

объяснить, почему отсутствие файлов не исключает вмешательства;

показать понимание различий между постоянными и временными артефактами.

Методический комментарий.
Кейс формирует представление о многоуровневой природе цифровых систем.

---

Кейс 3. «Мобильное устройство как связующее звено»

Исходная ситуация.
В ходе анализа инцидента выясняется, что пользователь активно использовал смартфон в момент подозрительных событий на рабочем компьютере.

Данные для анализа.
Имеются:

логическая копия данных мобильного устройства;

временная линия активности рабочей станции;

сведения о сетевых подключениях.

Задача обучающегося.
Определить возможную роль мобильного устройства в инциденте и предложить способы корреляции данных.

Ожидаемая логика рассуждений.
Студент должен рассматривать смартфон:

не как отдельный объект,

а как элемент общей системы взаимодействия.

Методический комментарий.
Кейс демонстрирует важность системного подхода и отказа от изолированного анализа.

---

Кейс 4. «Ложная причинность»

Исходная ситуация.
Временная линия показывает запуск неизвестного процесса незадолго до сбоя системы. Процесс был автоматически признан причиной инцидента.

Данные для анализа.
В наличии:

временная шкала событий;

сведения о назначении процесса;

данные о пользовательской активности.

Задача обучающегося.
Оценить корректность вывода и указать возможные ошибки интерпретации.

Ожидаемая логика рассуждений.
Обучающийся должен:

отличать временную корреляцию от причинной связи;

предложить альтернативные гипотезы;

показать необходимость проверки предположений.

Методический комментарий.
Кейс направлен на развитие критического мышления и осторожности в выводах.

---

Кейс 5. «Автоматизация против анализа»

Исходная ситуация.
Для анализа большого массива данных использованы ИИ-инструменты, автоматически выделившие «подозрительные» фрагменты.

Данные для анализа.
Результаты автоматической обработки и исходные данные.

Задача обучающегося.
Оценить роль автоматизации в анализе и определить, какие решения остаются за специалистом.

Ожидаемая логика рассуждений.
Студент должен:

понимать вспомогательный характер ИИ;

указать на риски некритического принятия автоматических результатов;

сформулировать границы ответственности специалиста.

Методический комментарий.
Кейс подчёркивает, что технологии усиливают анализ, но не заменяют мышление.

---

Методические рекомендации по использованию кейсов

Кейсы рекомендуется использовать в форме обсуждений, письменных аналитических заметок или коллективного разбора. Оценка должна базироваться не

---

Итог раздела «Учебная практика»

Учебные кейсы завершают практический блок статьи, переводя теоретические и инструментальные знания в плоскость анализа реальных ситуаций. Тако

---
---

## Заключение

Рассмотренный в статье материал демонстрирует, что анализ цифровых инцидентов не сводится к использованию отдельных программных средств или фо

В первой части статьи были обозначены основные классы инструментов, применяемых в цифровой криминалистике, инженерном анализе и расследовании

Раздел «Учебная практика» перевёл теоретические положения в плоскость реального применения. На примере анализа стационарных систем, мобильных

Отдельный модуль, посвящённый типовым ошибкам анализа, подчёркивает, что наибольшую угрозу качеству расследования представляют не технические

Учебные кейсы, включённые в практическую часть, ориентированы на формирование у обучающихся навыков аналитического мышления, а не механическог

В целом представленная структура демонстрирует, что цифровой анализ инцидентов является междисциплинарной инженерной задачей, находящейся на п

Материал статьи может быть использован как основа для учебных курсов, практических занятий, методических разработок и подготовки специалистов,

## Список использованных источников


1. Carrier B.
File System Forensic Analysis / B. Carrier. — Boston : Addison-Wesley Professional, 2005. — 800 p.

2. Casey E.
Digital Evidence and Computer Crime / E. Casey. — 3rd ed. — London : Academic Press, 2011. — 840 p.

3. Nelson B., Phillips A., Steuart C.
Guide to Computer Forensics and Investigations / B. Nelson, A. Phillips, C. Steuart. — 5th ed. — Boston : Cengage Learning, 2015. — 672 p.

4. Farmer D., Venema W.
Forensic Discovery / D. Farmer, W. Venema. — Boston : Addison-Wesley, 2005. — 432 p.

5. Ligh M., Case A., Levy J., Walters A.
The Art of Memory Forensics / M. Ligh et al. — Indianapolis : Wiley Publishing, 2014. — 912 p.

6. Sanders C.
Practical Packet Analysis / C. Sanders. — 3rd ed. — San Francisco : No Starch Press, 2017. — 368 p.

7. Bejtlich R.
The Practice of Network Security Monitoring / R. Bejtlich. — San Francisco : No Starch Press, 2013. — 480 p.

8. Hoog A.
Android Forensics / A. Hoog. — Amsterdam : Syngress, 2011. — 368 p.

9. Mojtahed V.
iOS Forensics / V. Mojtahed. — Birmingham : Packt Publishing, 2018. — 454 p.

10. Goodfellow I., Bengio Y., Courville A.
Deep Learning / I. Goodfellow, Y. Bengio, A. Courville. — Cambridge : MIT Press, 2016. — 800 p.

11. ISO/IEC 27037:2012.
Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence.

12. ISO/IEC 27041:2015.
Information technology — Security techniques — Incident investigation principles and processes.

13. ISO/IEC 27042:2015.
Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence.

14. ISO/IEC 27043:2015.
Information technology — Security techniques — Incident investigation.

15. NIST SP 800-86.
Guide to Integrating Forensic Techniques into Incident Response — Gaithersburg : National Institute of Standards and Technology, 2006.

16. NIST.
Mobile Device Forensics Guidelines — National Institute of Standards and Technology, USA.

17. The Sleuth Kit & Autopsy Documentation [Электронный ресурс]. — Режим доступа: https://www.sleuthkit.org (дата обращения: указывается при с

18. Wireshark User’s Guide [Электронный ресурс]. — Режим доступа: https://www.wireshark.org/docs (дата обращения: указывается при сдаче работы

19. Plaso / log2timeline Documentation [Электронный ресурс]. — Режим доступа: https://plaso.readthedocs.io (дата обращения: указывается при сд

20. Timesketch Documentation [Электронный ресурс]. — Режим доступа: https://timesketch.org (дата обращения: указывается при сдаче работы).

21. Praat: Doing Phonetics by Computer [Электронный ресурс]. — Режим доступа: https://www.praat.org (дата обращения: указывается при сдаче раб

22. Audacity Documentation [Электронный ресурс]. — Режим доступа: https://www.audacityteam.org (дата обращения: указывается при сдаче работы).

23. FFmpeg Documentation [Электронный ресурс]. — Режим доступа: https://ffmpeg.org/documentation.html (дата обращения: указывается при сдаче р